Evaluation Warning: The document was created with Spire.Doc for Python.

**FendPay（ 2.1.4.1版本）   
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。  
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | FendPay |
| 版本 | 2.1.4.1 |
| 包名 | com.pay.fend |
| 域名线索 | 24条 |
| URL线索 | 17条 |
| APP图标 |  |
| 分析日期 | 2025年6月18日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | GP00.apk |
| 文件大小 | 7.52MB |
| MD5值 | b9f8538475af980c86bfa572f3c2a66c |
| SHA1值 | 05315d85db45ead0eea8fcd138dfcc885b1855dc |
| SHA256值 | 47478a41d3cc73cfc1f14a4faf74bbd5b0987c1b240e3b3a37d2f11b3e9edbd7 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | FendPay |
| 包名 | com.pay.fend |
| 主活动Activity | com.pay.fend.FMainActivity |
| 安卓版本名称 | 2.1.4.1 |
| 安卓版本 | 2141 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| plus.google.com | IP: 210.209.84.142  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| download.lotteryluna.com | IP: 3.168.86.116  所属国家: United States of America  地区: Washington  城市: Seattle |
| download.btgamesbets.com | IP: 18.244.214.114  所属国家: United States of America  地区: California  城市: San Jose |
| file.bmob.cn | 没有服务器地理信息. |
| v0.api.upyun.com | IP: 218.28.104.157  所属国家: China  地区: Henan  城市: Zhengzhou |
| kspay.shop | IP: 104.21.96.1  所属国家: United States of America  地区: California  城市: San Francisco |
| download.mybtlottery.com | 没有服务器地理信息. |
| m0.api.upyun.com | IP: 218.28.104.157  所属国家: China  地区: Henan  城市: Zhengzhou |
| huidu-bucket.s3.ap-southeast-1.amazonaws.com | IP: 52.219.184.34  所属国家: Singapore  地区: Singapore  城市: Singapore |
| opentest.bmob.cn | 没有服务器地理信息. |
| p0.api.upyun.com | IP: 101.251.144.15  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| bt-games-sg.oss-accelerate.aliyuncs.com | IP: 8.131.131.67  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| pagead2.googlesyndication.com | IP: 114.250.64.38  所属国家: China  地区: Beijing  城市: Beijing |
| app.jdwe.pro | IP: 0.0.0.0  所属国家: -  地区: -  城市: - |
| schemas.android.com | 没有服务器地理信息. |
| download.garudalottery.com | IP: 163.181.228.144  所属国家: Singapore  地区: Singapore  城市: Singapore |
| p.bmob.cn | 没有服务器地理信息. |
| download.monsters789.com | IP: 3.167.212.18  所属国家: United States of America  地区: Washington  城市: Seattle |
| open.cctvcloud.cn | IP: 106.75.66.36  所属国家: China  地区: Shanghai  城市: Shanghai |
| io.codenow.cn | IP: 106.75.70.127  所属国家: China  地区: Shanghai  城市: Shanghai |
| 120.27.129.233 | IP: 120.27.129.233  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.freecharge.in | IP: 23.39.218.119  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| 47.243.17.51 | IP: 47.243.17.51  所属国家: United Kingdom of Great Britain and Northern Ireland  地区: England  城市: Manchester |
| spb-2481.jdwe.live | IP: 172.67.197.183  所属国家: United States of America  地区: California  城市: San Francisco |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://schemas.android.com/apk/res/android | R3/AbstractC0351b.java |
| https://plus.google.com/ | X1/J.java |
| http://p.bmob.cn/8/ | cn/bmob/v3/http/BmobURL.java |
| https://opentest.bmob.cn/8/ | cn/bmob/v3/http/BmobURL.java |
| https://open.cctvcloud.cn/8/ | cn/bmob/v3/http/BmobURL.java |
| http://file.bmob.cn | cn/bmob/v3/http/BmobURL.java |
| http://io.codenow.cn:3010 | cn/bmob/v3/http/BmobURL.java |
| http://m0.api.upyun.com | cn/bmob/v3/datatype/up/UpConfig.java |
| http://v0.api.upyun.com | cn/bmob/v3/datatype/up/UpConfig.java |
| http://v0.api.upyun.com/ | cn/bmob/v3/datatype/up/FormUploader.java |
| http://m0.api.upyun.com/ | cn/bmob/v3/datatype/up/BlockUploader.java |
| https://v0.api.upyun.com | cn/bmob/v3/datatype/up/ParallelUploader.java |
| http://p0.api.upyun.com/pretreatment/ | cn/bmob/v3/datatype/up/ParallelUploader.java |
| http://io.codenow.cn:3010/socket.io/1/ | cn/bmob/v3/realtime/Client.java |
| http://io.codenow.cn:3010/socket.io/1/websocket/ | cn/bmob/v3/realtime/Client.java |
| http://io.codenow.cn | cn/bmob/v3/realtime/Client.java |
| https://download.mybtlottery.com/app/GP00.apk | com/pay/fend/FMainActivity.java |
| http://120.27.129.233:5000/ | com/pay/fend/api/ApiConstant.java |
| http://47.243.17.51/prod-api/ | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/ | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/user/bindEmail | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/buy/order | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/usdt/buy | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/buy/order/cancel | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/tool/changeStatus | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/tool/changeSell | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/user/changeMinWithdrawAmount | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/user/checkBindPin | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/user/checkBindTg | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/user/checkPin | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/checkVersion | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/billsFilter | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/tool/details | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/bonusDetails | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/usdt/buy/details | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/home | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/tutorial | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/usdt | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/user/bindTgDetails | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/buy/order/simpleUserBank | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/bills | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/buy/order/listBuyOrders | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/usdt/pending | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/buy/order/details | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/sell/order/listUserSellOrders | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/tutorial/list | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/usdt/list | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/buy/order/listUserBuyOrders | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/tool/auth/step1 | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/tool/freeChargeAuth/step2 | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/tool/support | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/tool | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/user/mine | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/user/invite | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/user/login/otp | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/user/loginOut | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/user/login/pwd | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/buy/order/paid | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/usdt/submit | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/buy/order/submitUtr | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/user/register | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/user/setPin | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/user/update/pwd | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/uploadOSS | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/tool/deAuth | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/user/mentoring | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/buy/order/processOrderNo | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/customer/service | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/send/opt | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/user/receiveMentoring | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/user/bindEmail/sendOtp | com/pay/fend/api/ApiConstant.java |
| https://kspay.shop/app/tool | com/pay/fend/api/ApiService.java |
| https://download.mybtlottery.com/app/GP00.apk | com/pay/fend/activity/PersonalActivity.java |
| https://spb-2481.jdwe.live/ | com/pay/fend/activity/InfoWebActivityService.java |
| https://app.jdwe.pro/widget?website\_token | com/pay/fend/activity/InfoWebActivityService.java |
| https://www.freecharge.in/services | com/pay/fend/activity/AuthActivity.java |
| https://download.monsters789.com/home/Dear%20lottery.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/home/Kerala%20lottery.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/home/Mega%20Jackpot.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/home/Brilliant%20Night.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/home/5d%20dear.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/home/5d%20Kerala.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/games/scratchhome/wild1.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/games/scratchhome/wild.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/games/scratchhome/power.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/home/Wingo.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/home/K3.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/home/Quick%203D.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/pro-resource/2025/03/20/recharge\_20250320144441A011.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/pro-resource/2025/03/25/max\_20250325103005A001.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/pro-resource/2025/03/15/bd\_20250315104806A019.gif | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/pro-resource/2025/03/13/join\_20250313203526A009.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/pro-resource/2025/03/20/gscz\_20250320124010A009.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/pro-resource/2025/03/29/gs\_20250329091013A008.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/pro-resource/2025/03/04/SABA\_20250304144929A007.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/pro-resource/2025/03/04/Lucksports\_20250304144954A009.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/pro-resource/2025/03/04/TF\_20250304144938A008.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/pro-resource/2025/03/31/BTi\_20250331134112A011.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/home/Lucky%20Draw.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/home/Radiant%20Lottery.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/home/Golden%20Treasure.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/home/WIN-WIN.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/home/WEALTH%20BANQUET.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/home/STREE-SAKTHI.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/home/FIFITY-FIFTY.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/home/KARUNYA%20PIUS.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/home/NIRMAL.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/home/KARUNYA.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/home/AKSHAYA.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/games/scratchhome/wild3.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/games/scratchhome/goldmine.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/games/scratchhome/icecold.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/games/scratchhome/high.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/games/scratchhome/sapphire.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/games/scratchhome/triple.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/Rummy.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/TeenPatti-20-20.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/Jackpot-Fishing.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/Mega-Fishing.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/Callbreak-Quick.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/Caribbean-Stud-Poker.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/TeenPatti-Joker.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/Pool-Rummy.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/Callbreak.png | com/pay/fend/work/ImagePreloadManager.java |
| https://download.garudalottery.com/game/matka/Kalyan | com/pay/fend/work/ImagePreloadManager.java |
| https://download.garudalottery.com/game/matka/Kalyan.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.garudalottery.com/game/matka/Milan | com/pay/fend/work/ImagePreloadManager.java |
| https://download.garudalottery.com/game/matka/Main | com/pay/fend/work/ImagePreloadManager.java |
| https://download.garudalottery.com/game/matka/Satta | com/pay/fend/work/ImagePreloadManager.java |
| https://download.garudalottery.com/game/matka/Matka | com/pay/fend/work/ImagePreloadManager.java |
| https://download.garudalottery.com/game/matka/Fortune | com/pay/fend/work/ImagePreloadManager.java |
| https://download.garudalottery.com/game/matka/Destiny | com/pay/fend/work/ImagePreloadManager.java |
| https://download.garudalottery.com/game/matka/Luck | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/Royal-Fishing.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/cq9/Thai-HILO.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jdb/Fishing-Disco.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/Happy-Fishing.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/Bombing-Fishing.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jdb/Dragon-Fishing.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/MINI-FLUSH.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/Blackjack-Lucky-Ladies.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/Blackjack.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/Andar-Bahar.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/Pusoy-Go.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/Tongits-Go.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/AK47.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/TeenPatti.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/Ludo-Quick.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jdb/Dragon-Tiger-Joker-Bonus.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jdb/Dragon-Fishing-Ii.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jdb/Cai-Shen-Fishing.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/Ocean-King-Jackpot.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jdb/Shade-Dragons-Fishing.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/Dinosaur-Tycoon-II.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jdb/Fishing-Yilufa.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/All-star-Fishing.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jdb/Dragon-Master.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/Boom-Legend.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jdb/Fishing-Legend.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/Dragon-Fortune.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/Dinosaur-Tycoon.png | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/default/invite.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/pro-resource/2025/03/22/mfcp\_20250322143233A013.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.lotteryluna.com/pro-resource/2025/02/26/evolution\_20250226125723A005.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.garudalottery.com/game/casino/KM.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.garudalottery.com/game/casino/cq9.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.garudalottery.com/game/casino/T1.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.garudalottery.com/game/casino/LIve.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.lotteryluna.com/pro-resource/2025/02/26/Spribe\_20250226125658A004.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/pro-resource/2024/08/02/paytm\_20240802114021A002.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/pro-resource/2024/08/02/upi\_20240802114050A003.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/Money-Coming.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/Fortune-Gems.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/Fortune-Gems-2.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/Crazy777.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/Super-Ace.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jili/3 | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/pg/Fortune-Tiger\_app-icon\_rounded.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/pg/Fortune-Mouse\_rounded\_1024.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/pg/Rise-of-Apollo\_1024\_rounded.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/pg/Treasures-of-Aztec\_rounded\_1024.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/pg/Ganesha-Fortune\_rounded\_1024.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/pg/Wild-Bounty-Showdown\_1024\_rounded.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jdb/Mines.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jdb/Super-Niubi.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jdb/Plinko.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jdb/Elemental-Link-Fire.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jdb/Lucky-Seven.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/jdb/Treasure-Bowl.png | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/game/2j/ELVES.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/game/2j/MEDUSA | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/game/2j/GOLDEN | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/game/2j/MYTHICAL | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/game/2j/FORTUNE | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/game/2j/LUCKY | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/game/spire/Aviator.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/pro-resource/2025/03/05/Plinko\_20250305223716A017.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/game/spire/Balloon.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/game/spire/Keno%2080.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/game/spire/Mini%20Roulette.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/game/spire/Mines.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/games/t1/Niu | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/games/t1/Shoot | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/games/t1/Jungle | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/games/t1/SUPER%20777.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/games/t1/Lucky%2010.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/games/t1/Scratch | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/cq9/Xoc-Dia.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/cq9/Mr.Bean.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/cq9/Thai-Fish-Prawn-Crab.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/cq9/Tenfold-Eggs.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/cq9/Funky-Bingo.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/cq9/Jungle-Party.png | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/pro-resource/2025/03/25/7 | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/pro-resource/2025/03/25/3 | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/pro-resource/2025/03/25/ANDAR | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/pro-resource/2025/03/25/DRAGON | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/pro-resource/2025/03/25/TEEN | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/pro-resource/2025/03/25/AVIATOR | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/yeebet/Widow-Roulette-AR01.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/yeebet/Classic-Baccarat-EU01.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/yeebet/Violet-Baccarat-AB02.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/yeebet/Majestic-Bac-WB05.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/yeebet/Immortal-Roulette-ROU06.png | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/km/Game\_KMQM\_7\_Up\_7\_Down\_520x520.jpg | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/km/Game\_KMQM\_Poker\_Roulette\_520x520.jpg | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/km/Game\_KMQM\_Andar\_Bahar\_520x520.jpg | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/km/Game\_KMQM\_Coin\_Toss\_520x520.jpg | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/km/Game\_KMQM\_Triple\_Chance\_520x520.jpg | com/pay/fend/work/ImagePreloadManager.java |
| https://huidu-bucket.s3.ap-southeast-1.amazonaws.com/api/km/Game\_KMQM\_Elite\_Aviator\_Club\_343x200.jpg | com/pay/fend/work/ImagePreloadManager.java |
| https://download.btgamesbets.com/games/scratchhome/scratchtop/wild100.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.btgamesbets.com/games/scratchhome/scratchtop/wild.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.btgamesbets.com/games/scratchhome/scratchtop/power.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.btgamesbets.com/games/scratchhome/scratchtop/wild200.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.btgamesbets.com/games/scratchhome/scratchtop/goldmine.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.btgamesbets.com/games/scratchhome/scratchtop/icecold.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.btgamesbets.com/games/scratchhome/scratchtop/high.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.btgamesbets.com/games/scratchhome/scratchtop/sapphire.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.btgamesbets.com/games/scratchhome/scratchtop/tripe.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/games/matka/makad/1.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/games/matka/makad/8.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/games/matka/makad/7.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/games/matka/makad/6.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/games/matka/makad/5.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/games/matka/makad/4.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/games/matka/makad/3.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/games/matka/makad/2.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/games/matka/makad/10.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/games/matka/makad/9.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://bt-games-sg.oss-accelerate.aliyuncs.com/games/matka/makad/12.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.lotteryluna.com/config/spin/7.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.lotteryluna.com/config/spin/6.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.lotteryluna.com/config/spin/5.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.lotteryluna.com/config/spin/4.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.lotteryluna.com/config/spin/3.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.lotteryluna.com/config/spin/2.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.lotteryluna.com/config/spin/1.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.lotteryluna.com/config/spin/0.webp | com/pay/fend/work/ImagePreloadManager.java |
| https://download.monsters789.com/home/Dear%20lottery.webp | com/pay/fend/fragment/HomeFragment.java |
| https://pagead2.googlesyndication.com/pagead/gen\_204?id=gmob-apps | Q1/b.java |

### **4.3 邮箱线索**

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: CN=123, OU=123, O=123, L=123, ST=123, C=123 签名算法: rsassa\_pkcs1v15 有效期自: 2025-06-03 06:21:28+00:00 有效期至: 2055-05-27 06:21:28+00:00 发行人: CN=123, OU=123, O=123, L=123, ST=123, C=123 序列号: 0x1 哈希算法: sha256 md5值: 2d5cfe7915100c3580cbd32cf3a600d3 sha1值: 10843165d402be718c4ba303d50f4bcaa50b18b0 sha256值: 9c37ce86661f4c058010c6953b5a74afa6fd5f9b01182787be000a34cfcbb81b sha512值: 6b1c1d28970f2309a2f5e0220379903c4c8fa9e5bca1d8eca7eca205e03b75b32588a7d1267c5145bdae37a7c0d9ef052caf3198d9a26c996b9b3975a3af6b77 公钥算法: rsa 密钥长度: 2048 指纹: 49240be8cf9b37554a9097c597b61f6f22d70a45b686ae918f95185eac3b2911**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "enter\_password" : "Enter Password" |
| "google\_api\_key" : "AIzaSyDpFobGqlj3hxcwnxSdjKHyDX\_eY8C9wck" |
| "google\_crash\_reporting\_api\_key" : "AIzaSyDpFobGqlj3hxcwnxSdjKHyDX\_eY8C9wck" |
| "password" : "Password" |
| "permanently\_denied\_authorization\_please\_manually\_grant\_relevant\_permissions" : "Permanently denied authorization, please manually grant relevant permissions" |
| "please\_enter\_password" : "Please enter password" |
| "please\_enter\_your\_password" : "Please enter your password" |
| "repeat\_password" : "Repeat password" |
| "user" : "USER" |
| "enter\_password" : "पासवर्ड दर्ज करें" |
| "password" : "पासवर्ड" |
| "permanently\_denied\_authorization\_please\_manually\_grant\_relevant\_permissions" : "स्थायी रूप से अस्वीकृति, कृपया संबंधित अनुमतियाँ मैन्युअली प्रदान करें" |
| "please\_enter\_password" : "कृपया पासवर्ड दर्ज करें" |
| "repeat\_password" : "पासवर्ड दोहराएँ" |
| "user" : "उपयोगकर्ता" |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看 |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看 |  |  |

## **9. 此APP的危险动作**

| 向手机申请的权限 | 是否危险 | 类型 | 详细情况 |
| --- | --- | --- | --- |
| android.permission.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前 |
| android.permission.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| android.permission.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.ACCESS\_NETWORK\_STATE | 正常 | 查看网络状态 | 允许应用程序查看所有网络的状态 |
| android.permission.WRITE\_SETTINGS | 危险 | 修改全局系统设置 | 允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。 |
| android.permission.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |
| android.permission.LAUNCH\_APP | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.WAKE\_LOCK | 正常 | 防止手机睡眠 | 允许应用程序防止手机进入睡眠状态 |
| android.permission.CAMERA | 危险 | 拍照和录像 | 允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像 |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_EXTERNAL\_STORAGE | 危险 | 读取外部存储器内容 | 允许应用程序从外部存储读取 |
| android.permission.WRITE\_EXTERNAL\_STORAGE | 危险 | 读取/修改/删除外部存储内容 | 允许应用程序写入外部存储 |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| android.permission.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |
| android.permission.READ\_PHONE\_STATE | 危险 | 读取电话状态和身份 | 允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等 |
| com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VISUAL\_USER\_SELECTED | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_WIFI\_STATE | 正常 | 查看Wi-Fi状态 | 允许应用程序查看有关 Wi-Fi 状态的信息 |
| android.permission.REQUEST\_INSTALL\_PACKAGES | 危险 | 允许应用程序请求安装包。 | 恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。 |
| com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |
| com.pay.fend.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**